Internet et vie privée

Poullet, Yves

Published in:
Societa dell'informazione tutela della riservatezza

Publication date:
1998

presidente
PAOLO CASELLA
vice-segretario generale dell'Osservatorio
« Giordano Dell'Amore »

INTERNET ET VIE PRIVEE
Nouveaux enjeux, Nouvelles solutions

YVES POULLET
professeur à la Faculté
de Droit et au DES en Droit et Gestion
des Technologies de l'Information
et de la Communication de Namur - FUNDP;
directeur du CRID (Namur - Belgique)

Introduction

1. Notre propos est double:

— la première partie présente les "nouveaux" risques d'atteinte à la protection des données, risques liés au développement d'Internet, en particulier à l'interactivité qui caractérise ce réseau des réseaux. Cette interactivité permet en effet non seulement la collecte d'informations liées au comportement de l'utilisateur lors de ses diverses requêtes ou utilisations des services offerts par Internet, mais également des collectes supplémentaires à partir de programmes introduits à l'insu de l'utilisateur dans le système d'informations de ce dernier.

— la seconde partie recherche les solutions "nouvelles" apportées à ces risques. La technologie et l'autorégulation fournissent en la matière des solutions indispensables pour assurer l'effectivité des dispositions réglementaires. Leur analyse ouvre une discussion sur la complémentarité voire la substitution des solutions non réglementaires à celles réglementaires privilégiées par l'Europe. On souligne en particulier le surcroît de "maîtrise" que les solutions techniques offrent à l'utilisateur. Enfin, Internet invite à relire les dispositions réglementaires de la Directive pour s'assurer du caractère "adéquat" de la protection qu'elle prétend garantir.

Ndr: L'auteur remercie particulièrement Monsieur Jean-Marc Dinant pour les multiples informations, conseils et réflexions prodigués lors de la rédaction de ces pages dont certaines reprennent in extenso sa propre prose.

Les recherches menées ici s'inscrivent dans le cadre des études menées par le pôle d'interuniversitaire "Société de l'information" qui regroupe la CITA, le CRID des FUNDP, le LENTIC de l'Ulg et le SMIT de la VUB (Brussels) financépar les S.S.T.C., administration de l'État belge.

IÈRE PARTIE: INTERNET, DE "NOUVEAUX" RISQUES

2. Cette première partie examine les risques d'atteinte à la protection des données, lors de l'utilisation d'Internet. Ces risques se déduisent aisément des caractéristiques de ce réseau des réseaux qu'est Internet (I); ils se conçoivent aussi par l'absence de transparence du fonctionnement d'un réseau qui en aucune manière ne peut être réduite à une application simple du modèle d'architecture "client/serveur" (II).

I. *De quelques caractéristiques d'Internet*

3. Internet, ce réseau des réseaux, présente des caractéristiques qui justifient l'attention particulière des défenseurs de la vie privée:

— réseau ouvert: la connexion au réseau et son utilisation sont aisées grâce à des protocoles simples [1]. L'ouverture du réseau explique largement le succès d'Internet mais également les risques liés à l'absence de contrôle des entrants sur le réseau et la possibilité pour eux d'y lire les messages y circulant [2]. Si le cryptage des messages apparait comme une solution à de tels risques [3], on conçoit également que sans attendre, des entreprises ou organisations [4] aient développé des réseaux fermés fondés sur les mêmes protocoles que ceux d'Internet, réseaux dits Intranets. La connexion des Intranets avec Internet est alors l'objet de contrôles assurés par des "Firewalls".

L'ouverture des réseaux, la libre accessibilité de tous et chacun à des messages circulant sur le réseau ou à des informations mises à la disposition du public font craindre des détournements de finalités de ces messages ou informations. Ainsi; un internaute pourra, et des logiciels tels Yahoo, Altavista, ... l'y aideront, repérer les multiples manifestations d'expression de tel ou tel personnage pour mieux en cerner le profil type et prendre telle ou telle décision vis-à-vis d'elle. On citera à ce propos le logiciel Deja News qui permet de retracer les différents newsgroups auxquels une personne a déjà participé [5].

4. — réseau interactif: si certains serveurs rassemblent de larges banques de données personnelles, bibliographiques, liste d'étudiants, de chercheurs ou de professionnels [6], annuaires téléphoniques [7], la question de la protection des données s'entend également des données créées consciemment ou inconsciemment par l'internaute lorsqu'il utilise sa connexion et en particulier, lorsqu'il visite les sites de la toile (Web).

Nous reviendrons plus tard (infra, n. 6) sur les traces inconscientes laissées par l'internaute, relevons simplement que chaque internaute dispose d'une adresse I.P. [8], conférée par le fournisseur d'accès, que cette adresse est véhiculée [9] lors de chaque requête auprès d'un site ou lors de l'envoi d'un message en de multiples endroits c'est-à-dire, outre au lieu de destination, dans chaque ordinateur qui participe à l'acheminement du message.

Au-delà, il va de soi que suite à l'accès à un site particulier, l'internaute qui a peut être revélé son nom et son adresse, livre de l'information non seulement par le contenu des messages qu'il adresse, mais également par la façon dont il consulte les pages du site, le temps consacré à la lecture de telle ou telle page, le site de provenance et celui vers lequel il s'oriente. Autant d'informations qui permettent au serveur de mieux connaître les goûts et les habitudes de consultation de l'internaute qui s'adresse à lui.

5. — réseau international: Les spécialistes annoncent la connexion de 16,5 millions de machines à Internet [10], machines réparties sur tous les continents. La réalité internationale du réseau invite à quelques considérations sur les protections offertes par le droit dans les diverses parties du monde. Si la directive européenne de protection des données offre un haut niveau de protection des données, la protection y offerte ne risque-t-elle pas d'être aisément détournée par l'implantation hors Europe d'un site? La question est d'autant plus cruciale que la délocalisation d'un site est chose aisée et que dès lors, on peut imaginer qu'un serveur, pour échapper aux règles protectrices européennes, ouvre son site hors de frontières européennes. Nous reviendrons sur les dispositions prises par la directive en matière de flux transfrontières, dispositions qui trouvent certainement à s'appliquer dans le cas de flux liés à l'utilisation d'Internet mais dont l'effectivité dans la pratique est loin d'être évidente.

II. *De la face cachée d'Internet: les traitements dits invisibles*

6. Une récente analyse de J-M. Dinant, informaticien à la Commission belge de protection de la vie privée et chercheur aux Facultés Universitaires Notre-Dame de la Paix [11] s'attachait à montrer les multiples processus susceptibles de créer des

[1] Il est remarquable de noter que la normalisation de certains protocoles utilisés dans Internet s'est faite en dehors de tout organisme officiel de normalisation, au sein d'une structure au départ informelle qui par la suite s'est organisée, soit au sein de l'IETF (Internet Engineering Task Force).

[2] Ainsi, l'agence Belga, les 27 et 28 janvier 1997, dénonçait l'accès de surfers non autorisés à des données bancaires. En l'occurrence, une banque avait autorisé ses clients utilisateurs d'Internet, à opérer « en toute sécurité », des opérations bancaires via Internet.

[3] Cf. à ce propos, nos réflexions infra, n. 23.

[4] Ainsi, même des universités, lieux de naissance du réseau ouvert qu'est Internet, développent aujourd'hui des Intranets. La Chine a développé de même à un niveau national, un réseau Intranet connecté au reste du monde par des "gateways" situés aux frontières et ce par crainte de la "contamination culturelle" (cf. à ce propos, J. CHU, *In a borderless Cyberspace*, I.T. Magazine, Special Internet, p. 95 et s.

[5] A noter la clause d'irresponsabilité insérée par les promoteurs du site: « Our Author Profile is a great way to get insight into an author's Usenet presence and find out what he/she is interested in. Indexing errors however though rare can occur ... we are not liable for inaccuracy... » Deja News Author Profile, http://xp7.deja news.com/profile.

[6] A propos de ces deux exemples et de bien d'autres, A. MOLE, *Deux avis de la CNIL relatifs à la diffusion de données nominatives sur Internet: une application anticipée de la directive communautaire*, DIT, 1996, n. 2, p. 62 à 64.

[7] Ces sites permettant de retrouver le numéro de téléphone à partir de l'identité de la personne sont l'objet de l'attention de plusieurs commissions de protection des données (ainsi, en Belgique, R.F.A, etc.).

A propos de ces sites, nos réflexions in C. de TERWANGNE et Y. POULLET, *Les annuaires téléphoniques au carrefour de droits*, I.T., 1996.

[8] ... distincte de son adresse électronique, dans la mesure où l'adresse I.P. peut ne pas être permanente et être conférée par le fournisseur d'accès lors de la demande d'un client d'accèder aux sites Web.

[9] Sauf à utiliser la technique du "remailing " (cfr. infra n. 24). Sur cette technique, C.A. GIMON, *World's Most Popular Remailer Closes*, article consultable à l'adresse suivante: http//www.info.nation.com/penetic.html. Cet article relate l'injonction adressée par la cour d'appel d'Helsinki, le 20 septembre 1996 à J. Helsingius de révéler le nom d'un utilisateur ayant violé la protection des droits d'auteur et ayant utilisé la protection des droits d'auteur et ayant utiliséles services d'anonymisation procurées par le site "anom.penet.fi" créépar Helsingius. Depuis ce site est fermé. Sur le ramiling, lire également A. BACARD, *Anonymous Remailer Faq*, disponible à l'adresse suivante: http://www.well.com/user/abacard/remail.html.

[10] Soit une augmentation de plus de 35% au cours de 1996. La population des internautes est elle évaluée à 80-100 millions (800 millions à 1 milliard prévus en 2001).

[11] J-M. DINANT, *Les traitements invisibles sur Internet*, papier présenté à la conférence du GERI

traitements à l'insu de l'utilisateur moyen naviguant sur Internet et d'affecter dès lors sa vie privée.

L'auteur y combattait une vision "naïve" d'Internet, conçu comme une hyperbibliothèque, fondée sur une architecture client/serveur et qui dès lors n'engendrerait à partir d'une structure permanente que les transactions demandées par l'utilisateur.

Deux catégories de traitements invisibles sont possibles: la première touche les couches de base (essentiellement les couches transports 1, 2 et 3 du modèle ISO); les autres sont liés aux applications qui fonctionnent à partir des couches supérieures (4,5,6,7) du modèle ISO.

A. *Traitements invisibles et couches inférieures*

7. Le premier risque de traitement invisible est lié au routage des messages électroniques. Même pour un courrier électronique national [12] la voie empruntée par le message peut suivre des chemins étrangers qui l'amènent dans des pays lointains où les opérateurs mal intentionnés pourraient noter les adresses I.P. de provenance le nom des intervenants s'il est en clair voire une copie du message.

Le deuxième risque de traitement invisible résulte des manipulations possibles des adresses équivalentes au "nom de domaine" (Domain Name Server). Le fait d'entrer une adresse reprenant le nom de domaine [13] ne signifie pas que l'on accède au site de ce domaine. Dans les faits, le serveur ou un tiers peuvent router le message vers une page venant d'un autre site ou à une page "aménagée" du site voulu [14].

On signale enfin, la commande PING qui permet de s'assurer à l'insu du destinataire que la machine de celui-ci est connectée.

B. *Traitements invisibles et couches supérieures* [15]

8. J-M. Dinant distingue quatre techniques permettant des traitements dits invisibles.

— les scripts CGI,
— les cookies,
— les scripts JAVA,
— les applets JAVA.

"L'ordre dans lequels ces techniques sont présentées n'est pas innocent. Il s'agit d'un ordre chronologique (avec une réserve pour l'ordre des deux premières techni-

(Groupe des commissaires européens de réflexion sur Internet réuni à Paris des 2 et 3 avril 1997), texte disponible à l'adresse suivante http://www.det.fundp.ac.be/ jmdi.

[12] L'auteur prend le cas d'un courrier envoyé de Namur à Bruxelles (65 km) qui quitte la Belgique, pour la Suisse, la France, la Suède et la Finlande.

[13] Par nom de domaine, on entend la requête placée dans l'en-tête du message: par ex. http://www.research.att.com/ presnik/papers/fte96/testimony.htm. que l'on peut décomposer comme suit:
— http: protocole du web
— www.research.att.com: adresse de la machine
— presnik/papers/ftc96/testimony: parmi les fichiers "testimony" présentés à la "Federal Trade Commission", le paper de Mr. P. Resnick.

[14] Ainsi, par exemple, 3 suisses, en fonction de la connaissance qu'il a de l'utilisateur renverra non seulement au site du pays de l'utilisateur mais en outre à un enchaînement de pages que la firme estime "intéressantes" pour l'internaute.

[15] Nous reprenons ici le texte de J-M Dinant afin de ne point corrompre par des mots impropres la rigueur technique de son propos. Nous avons ajouté un certain nombre d'informations complémentaires en note.

ques) mais, aussi et surtout, d'une gradation dans l'opacité des traitements effectués et, parallèlement, dans la perte, par l'utilisateur du navigateur, de la maîtrise tant des traces qu'il laisse lors de la consultation que de l'information elle-même à laquelle il accède.

Le point commun de ces quatre techniques est qu'elles permettent une dynamisation et un polymorphisme de l'espace informationnel dans lequel l'utilisateur évolue.

Par ailleurs, ces techniques ne sont pas exclusives l'une de l'autre. Un navigateur montrant une même page HTML, peut par exemple appeler un script CGI, recevoir et stocker un cookie, exécuter quelques instructions en JavaScript et un applet JAVA".

a. Les scripts CGI

— De quoi s'agit-il?

9. "Les scripts CGI utilisent une particularité du langage HTML, dans lequel sont écrites les pages du WEB. Il s'agit de l'option "FORM". Cette option permet à l'utilisateur de remplir certains champs à l'écran et d'ensuite les transmettre à un serveur pour traitement. Dans ce script, figure le nom d'un programme qui traitera les données transmises du site client" vers le site serveur.

— Quels sont les risques?

10. "Bien souvent, l'utilisateur sera invité à remplir un certain nombre de données à caractère personnel en échange d'un cadeau. Cette technique est déjà largement utilisée par les sociétés de mailing et la personne concernée n'a que rarement conscience que le cadeau qu'elle reçoit n'est que le prix de la transmission de ses propres données...

De par les spécifications des scripts CGI, le site serveur peut facilement connaître, lors de la soumission du formulaire les renseignements suivants:

1. l'adresse IP;
2. le type du processeur de la machine utilisée par le navigateur;
3. la dimension de l'écran du navigateur (en pixels);
4. le nombre de couleurs possibles à l'écran;
5. le type de navigateur;
6. la version du navigateur;
7. la langue acceptée par l'utilisateur (dans certains cas).

Ici encore, cette transmission d'informations entre le client et le "serveur" a lieu de manière invisible et est possible grâce à certains protocoles qui se matérialisent par une série de sous-programmes présents sur la machine hébergeant le navigateur".

b. Les cookies

— De quoi s'agit-il?

11. « Les cookies sont des informations persistantes enregistrées sur la machine du client Internet. Leur apparition n'a rien de "vicieux" (au sens juridique du terme) en soi et constitue en substance une conséquence logique de l'existence de formulaires CGI: le serveur a besoin, dans un certain nombre de cas, de pouvoir iden-

tifier qu'il a "en face" de lui, la même personne [16]. Pour ce faire, il peut envoyer un cookie (ou plusieurs) au navigateur. Il s'agit d'un paquet d'informations contenant:

1. le nom du cookie
2. sa valeur (souvent incompréhensible)
3. sa date d'expiration.

Le navigateur recevant un cookie le stocke dans un fichier particulier situé sur la machine de l'utilisateur et y rajoute le nom de l'ordinateur serveur duquel il a reçu l'information.

Par la suite, si la date d'expiration du cookie n'est pas atteinte, le navigateur le communiquera systématiquement lors de chaque requête HTTP (concrètement lors de chaque accès à une nouvelle page du WEB) si le serveur appartient à la même famille (au niveau DNS) que le serveur ayant transmis la valeur initiale du cookie. Dans sa réponse l'ordinateur serveur peut modifier la valeur du cookie ou sa date d'expiration ou renvoyer des cookies supplémentaires. Il peut aussi le supprimer (en lui donnant une valeur nulle) ».

— Quels sont les risques?

12. « Certains risques ont été rapportés par le CERT [17]: "Les cookies sont des informations que le serveur stocke sur le disque de l'utilisateur sans que celui-ci soit prévenu. Le serveur peut également interroger le fichier de cookies qui se trouve sur le disque dur de l'utilisateur. Cette fonctionnalité s'apparente un peu à la petite mémoire que possèdent les Minitels [18]. Mais le serveur peut également récupérer l'historique des pages WEB que vous avez consulter. Cette fonctionnalité est utilisée par les sociétés de marketing direct pratiquant le "one-to-one marketing" [19] afin de ci-

[16] L'utilisation des cookies se justifie comme suit:

— soit, il s'agira (on line ordering systems) qui permet d'enregistrer les achats ou transactions déjà réalisés auprès d'un site et qui vous permettra de les retrouver aisément;

— soit il s'agira de permettre une personnalisation de la visite du site qui a fait l'objet de visites préalables, par exemple si lors de la première visite, vous avez refusé de ne pas regarder les annonces commerciales mais vous êtes concentrés sur telle ou telle page, le cookie vous permettra d'être la prochaine fois guider vers les pages d'intérêt pour vous;

— enfin, le cookie peut permettre de connaître les autres sites que vous fréquentez (web site tracking). Cette technique est utilisé par les serveurs d'annonces comme IMGIS et double click. (Sur ces différents points, Andy's Netscape http Cookies notes (http://www. illuminatus/com/cookie. fcgi)).

A propos des cookies, lire les spécifications à l'adresse technique: http://www.netscape.com/newsref/std/cookie—spec..html.

[17] Rapport disponible à l'adresse:htt://www.sur.fr.net/ce/090796-7html.Sur les cookies, lire également: Andy's Netscape HTTP cookie Notes disponible à l'adresse suivante: http://www.illuminatus/com/cookie.fcgi; Malcom's Guide to persistent cookies resources, disponible à l'adresse suivante: http://www.emf.net/ mal/cookiesinfo.html.

[18] Les premiers Minitels disposaient en effet d'une mémoire vive qui enregistrait les utilisations faites par les usagers. Suite à une plainte des associations de consommateurs et d'une action de la CNIL, France Télécom avait supprimé ces possibilités de la série suivante de Minitel.

[19] On notera à ce propos, le système proposé par Double Click, "the premier Internet Advertising network" (pour la présentation de ce système, consulter le site: http://www.doubleclick.com) Double click propose à des entreprises ou groupes d'entreprises un service de profilage de clientèle par l'enregistrement d'informations relatives à l'utilisation du navigateur des personnes visitant un des sites des entreprises.

Le système DoubleClick ne crée pas de banque de données nominatives externes au système d'informations de l'utilisateur mais met en place sur le disque dur des cookies qui permettront aux sites visités de repérer immédiatement les aires d'intérêt de l'utilisateur afin de le conduire aux pages adéquates. C'est en ce sens que DoubleClick peut écrire: "Internet user privacy is a paramount concern of the DoubleClick network... The DoubleClick Network does not track or store users by their individual names a email adresses. No names are known, so no names are marketed or sold".

bler les utilisateurs et d'enregistrer dans des bases des profils précis d'habitudes, reflexes, goûts et centres d'intérêts dans le but de générer dans les pages Web que consulte l'utilisateur des publicités très ciblées. Cela pose un important problème de respect de la vie privée...".

Le système des cookies permet en effet le "one to one marketing". Ainsi, des sociétés comme DoubleClick opèrent leurs activités sur base de tels cookies. Des sociétés adhèrent à DoubleClick et permettent à cette société de mettre des espaces publicitaires sur les pages de leurs propres sites. Ces pages stockent des appels de télédéchargement de bannières publicitaires [20] à partir du site de DoubleClick. Chaque fois que l'internaute accède à une telle page, DoubleClick sélectionne la publicité adéquate en fonction du profil de consommation de l'internaute, profil déduit des choix préalables stockés sur un cookie installé sur le disque dur de l'internaute. La bannière publicitaire envoyée et les références du site visité (voire la page précise y choisie) sont reprises par DoubleClick qui modifiera en ce sens le cookie de l'internaute. Si l'internaute clique sur la bannière publicitaire, l'accès au site par l'Internaute s'opèrera via Double Click qui enregistrera bien évidemment l'intérêt de l'Internaute pour le produit concerné.

"Pour être averti du passage des cookies, l'utilisateur peut effectuer un paramétrage du navigateur. Mais les avertissements du passage de cookies deviennent à la longue épuisants et sont de toute façon inintelligibles car ils sont codés.

Enfin, il faut signaler, qu'en pratique, la date d'expiration de ces cookies est souvent très lointaine. Cette technique permet donc de marquer un utilisateur particulier avec certaines données qui le concernent et dont la signification est tout à fait hermétique. On pourrait donc inclure dans ces cookies des données sensibles que l'on aurait pu déduire de certaines réponses à des formulaires envoyés précédemment".

"En d'autres termes, si un jour un site Internet (moyennant une programmation adéquate) arrive à la conclusion qu'un utilisateur est juif, il pourra coller une étoile codée sur le dos de cet utilisateur de telle manière que chaque site de sa famille de ce site puisse avoir vent de cette caractéristique ».

c. Les Scripts Java

— De quoi s'agit-il?

13. "Lorsqu'un navigateur reçoit une page d'un site, cette page peut contenir certaines instructions en JavaScript. Ces instructions sont interprétées en temps réel par un interprétateur JAVA [21] intégré dans ou appelé par le navigateur. Typiquement, l'exécution de ces micro-programmes écrits en langage JavaScript a pour effet de dynamiser la page affichée en effectuant certaines animations ou en liant l'exécution de certains micro-programmes à certains boutons particuliers présents dans la page".

— Quels sont les risques?

14. "Il semble certain à l'heure actuelle que plusieurs trous de sécurité [22] existaient dans le langage JavaScript lorsqu'il était interprété par les versions 2.0. et 2.1.

[20] DoubleClick prétend avoir déjà produit plus de 400 millions de bannières. Elle a créé différentes sociétés en Europe.

[21] Java is a small simple object oriented programming language that is attracting a lot of interest for use on the W.W.W. » (M.I.T. lab for computer science: Summer Seminar Series: http://sls www. lcs.mit.edu/-hurley/sss. html). Ces trous de sécurité permettraient des manipulations sur le disque dur de l'utilisateur (cf. à ce propos les réflexions http://www.csprinceton.edu/sip/News.html).

[22] Le 23 février 1996, I.T. networks (Information for I.T. Professional disponible à l'adresse sui-

du navigateur Netscape. Il semblerait que certaines pages auraient eu pour effet de transmettre au serveur appelé des fichiers se trouvant sur le poste client (à l'insu, bien sûr de l'utilisateur), voire de les modifier. Toutefois, aucune attaque de ce type n'a été rapportée, bien que la possibilité technique ne semble plus faire aucun doute au niveau théorique. Si certains problèmes de protection des données ont été résolus dans les versions ultérieures, il n'en demeure pas moins que de nouveaux problèmes surgissent sans cesse".

d. Les Applets Java

— De quoi s'agit-il?

15. "Il s'agit d'une évolution des scripts JAVA à ne pas confondre avec ces derniers. Dans le cas des applets, les instructions JAVA sont préalablement traduites dans un pseudocode par les soins d'un précompilateur installé sur le serveur. Lors de l'exécution d'un applet, le navigator charge le Pcode lié à l'applet et l'exécute par le biais d'un inteprétateur livré par SUN (propriétaire du langage JAVA)".

— Quels sont les risques?

16. "La différence fondamentale entre les scripts et les applets est que les premiers sont transmis en langage clair au navigateur tandis que les seconds sont préalablement converti en Pcode et donc inintelligibles, même pour un programmeur moyen. Dans les deux cas de figure, la transmission s'effectue de manière souterraine mais, ici encore, la possibilité existe, dans les navigateurs récents d'inhiber l'exécution des scripts ou des applets.

Toutefois une telle solution a pour effet de bord de désactiver toute l'animation possible des pages html, rendant ainsi leur consultation plus morne, voire impossible à assurer la protection non seulement du contenu des messages mais en outre et surtout des données "transactionnelles" résultant de l'utilisation même des sites.

Aux risques ainsi identifiés, s'en ajoutent d'autres moins facilement identifiés et liés soit à l'absence de transparence du fonctionnement du réseau ou de certitude du réel destinataire, soit à la possibilité dans un réseau interactif de loger dans le système de l'utilisateur, quelques repères voire quelques programmes qui à l'insu de l'utilisateur ajouteront ou affineront les informations transmises par ce dernier lors de la visite d'un site".

Conclusions de la première partie

17. L'utilisation des multiples fonctionnalités du réseau Internet, accentue les risques d'atteinte à la protection des données, de par les caractéristiques du réseau:

— l'ouverture du réseau et les grandes facilités de réutilisation des données y circulant suscitent les craintes d'utilisations des données incompatibles avec la finalité qui a présidé à l'envoi du message. En outre, l'ouverture du réseau rend incontrôlable la circulation des informations et leurs utilisateurs;

— l'internationalisation des flux favorisée par la large diffusion du standard Internet et par le faible coût d'utilisation de ce réseau génère la peur de voir la protection proposée par certaines réglementations s'évanouir au fil des chemins lointains parcourus par les messages;

— enfin, l'interactivité du réseau et surtout son mode de fonctionnement par hyperliens justifient l'attention portée aux risques liés au traçage des utilisations du www.et aux possibilités infinies d'espionnage que l'envoi de programmes sur le système d'informations de l'utilisateur permet.

vante: http://www.itworks.be/1-update/week0896.html) écrivait: "If you really don't want others to run programs on your computer while you are browsing the Net. either don't use a Java compatible browser, or turn Java off in the security preferences". JavaScript compatible browsers like Netscape 2.0. allow you to include JavaScript code in your HTML page. With it, you can do all sorts of things to the unaware surfer who uses Netscape 2.0. An example is at http://www.popco.com/grabtst.html. If you access the page from Nescape 2.0., your browser will automatically send email to an automatic replyer at popco.com. This softbot will send you an email back to prove that it really grabbed your email address. In fact, the mechanism is extremely simple, and we will definitively find it in thousands of Web pages soon. There is only one thing you can do aganist it: put a bogus email address in your browser's email reply entry, or leave it blank".

Deuxième partie: INTERNET, DES SOLUTIONS

18. Avant d'aborder la solution réglementaire à la lumière de l'application de la Directive (I) la deuxième partie analyse les solutions que pourraient apporter l'autorégulation et les mesures techniques (II) dont l'effectivité est sans doute plus grande même si d'emblée, on souligne que leur mise sur pied et leur contenu seront souvent dictés par la pression réglementaire qui de ce fait reste, à notre avis, indispensable.

La seconde partie analyse deux grandes catégories de solutions: les solutions techniques et d'autoréglementation, d'une part, celles réglementaires d'autre part.

La première catégorie de solutions, objet de la section I, naît du développement même du réseau, ce qui en fait l'inestimable valeur dans la mesure où ces solutions sont élaborées au "niveau le plus adéquat" [23], là où surgissent les problèmes. Leur effectivité est d'autant plus forte que leurs concepteurs sont les acteurs même du réseau et que leur efficacité, dans cette mesure, dépasse les frontières.

19. Ces solutions sont indispensables, sont-elles suffisantes? M-H. Boulanger et C. de Terwangne en affirmaient les limites dans les termes suivants [24]: « Ces solutions dans la mesure où elles sont fondées sur le volontariat de ceux qui sont amenés à les adopter et à les mettre en oeuvre, leur caractère effectif peut être sérieusement mis en cause. ...(elles) ne sont soumises à aucune publicité organisée et ne tiennent compte que dans une certaine mesure de l'intérêt des individus. En effet, même si leurs rédacteurs sont souvent conscients de la necessité d'assurer une protection des personnes concernées par les données, ils la traduisent selon leur propre logique, généralement sans qu'un débat réunissant tous les intéressés n'ait eu lieu... L'autoréglementation par son caractère trop souvent unilatéral et par les choix techniques a priori qu'elle pose, présente le défaut de ne pas véritablement opérer une balance des intérêts contradictoires en présence... ».

Ensuite et surtout, en matière de protection des données, tout n'est pas négociable. Si comme nous le verrons les mesures techniques permettent sans conteste d'ac-

[23] Sur cette idée, P. Trudel, *Le cyberspace: réseaux constituants et réseau de réseaux*, in *Les autoroutes de l'information: enjeux et défis*, n. 39, Lyon, *Les chemins de la Recherche*, 1996, p. 192 et s. Cf. également "It is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop design principles for I and C; Technology and multimedia hard and software which will enable the individual user to control and give him feedback with regard to his personal data....".

(Intern. Working Group on Data Protection in Telecommunications, Data Protection and Privacy on the Internet, Report and Guidance, 19 nov. 1996, dit Budapest-Berlin Memorandum.

[24] M-H. Boulangier et C; de Terwangne, *Internet et le respect de la vie privée*, in *Internet face au droit*, E. Montero (éd.), Cahier du CRID, n. 12, p. 195.

croître de manière sensible la maîtrise de l'individu sur la circulation de son image informationnelle, cette maîtrise même toute puissante ne peut être le fondement unique et suffisant des traitements. La légitimité de ceux-ci reste requise et elle ne peut se déduire du seul consentement de la personne concernée. Nous reviendrons sur cette assertion.

20. Dans la mesure où la législation apporte la garantie de cette balance d'intérêts et fonde la légitimité des traitements sur une telle balance, il nous apparait nécessaire d'analyser dans une seconde section, l'applicabilité de la Directive 95/46 CE du Parlement européen et du Conseil du 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.

Il s'agira essentiellement à la fois de montrer combien le phénomène Internet interpelle la Directive et à la fois, d'analyser la qualité des solutions qu'elle apporte aux questions suscitées par le développement de ce phénomène.

Section 1: *Les solutions techniques et d'autoréglementation*

21. Nous ne nous attarderons pas sur les différentes solutions autoréglementaires classiques, qu'ils s'agissent des « Netiquette » ou des « Acceptable Use policies'' dont certaines contiennent des dispositions précises en matière de respect de la vie privée. Nous n'aborderons pas non plus les diverses techniques qui permettent vaille que vaille d'assurer leur respect, ainsi le « flaming », le « spamming »voire les bombes à destination de la boîte aux lettres du site indélicat. [25].

22. Diverses solutions techniques sont généralement avancées [26]. Elles répondent à des soucis divers. Les premières visent à garantir la confidentialité des messages exprimés par les utilisateurs; les deuxièmes, à garantir ce dernier contre les intrusions venant de l'extérieur; les troisièmes, contre les pratiques des destinataires des messages. En ce sens, elles sont complémentaires. Les premières tournent autour de l'encryptage, qu'ils s'agissent de l'encryptage lui-même, du remailing ou la possibilité de surfing anonyme (A), les secondes combattent les traitements invisibles dont nous avons parlé dans la première partie (B), les troisièmes enfin, utilisent la technologie PICS pour contrôler les pratiques des serveurs en matière de vie privée (C).

A. *Les techniques d'encryptage*

23. ''The use of secure encryption methods must become and remain a legitimate option for any user of the Internet'', c'est en ces termes que le Group de Berlin [27] affirmait le droit de l'utilisateur d'Internet à bénéficier d'une protection de ses données vis-à-vis des multiples acteurs appelés à intervenir dans le transport de son message voire même vis-à-vis de son destinataire.

[25] Sur ces différentes formes d'autoréglementation, lire C. Lamouline et Y. Poullet, *Les libertés individuelles et les autoroutes de l'information*, Rapport au Conseil de l'Europe, mai 1996, Bruylant, éd. Némésis, Bruxelles, à paraître.

[26] A propos de ces diverses solutions techniques, L.F. Cranor, *The role of technology in Self regulatory Privacy Regimes*, Paper prepared for the NTIA, Déc. 1996.

[27] Il s'agit de l'International Working Group on Data Protection in Telecommunications créé par la Conférence Internationale des Commissaires à la Protection des données. Ce groupe a émis le 19 novembre 1996 à sa 20. session un ''Data Protection and Privacy on the Internet'' - Report and Guidance'' dit Budapest-Berlin Memorandum.

Au-delà de l'encryptage qui consiste à rendre des messages digitaux illisibles [28], on évoque les systèmes des remailings et les techniques de surfing anonymes.

24. Le remailing permet à l'utilisateur d'envoyer des messages électroniques sans révéler son identité. Deux types de remailers existent; le Pseudo anonymous remailer [29] et l'anonymous remailer. Dans le premier cas, ''la personne qui veut rester anonyme adresse une requête auprès du serveur d'anonymisation. Celui-ci accorde un faux' email account' qui correspond avec sa vraie adresse email. De tous les messages que l'utilisateur envoie à ce serveur, l'entête sera supprimée et remplacée par une nouvelle qui contient les informations de la fausse adresse. De plus, certains serveurs soutiennent l'encryptage de façon qu'on peut dissimuler le contenu face au gérant du serveur'' [30].

Dans le système proposé par les anonymous remailers aucune trace relative à l'utilisation du remail service n'est conservée. On distinguera les Cypherpunk remailers [31] et les Mixmaster remailers [32].

Le surfing anonyme permet à l'utilisateur d'éviter que les serveurs avec qui il entre en contact puisse garder des informations concernant son processeur, son programme de navigation, son adresse IP et le dernier site visité. Il repose sur le principe suivant: au lieu de télédécharger immédiatement des fichiers HTML auprès du serveur en question, on se met d'abord en contact avec un serveur d'anonymisation qui télédécharge le document pour l'utilisateur. Ce serveur fonctionne donc comme client du premier serveur. Les protocoles d'application qui sont soutenus ainsi sont: http, ftp, news, gopher... [33].

[28] Ainsi le PGP (Pretty Good Privacy) développé par Zimmermaun. Les algorithmes de chiffrement utilisés sont surtout le DES (Data Encryption Standard) (clé de 56 bits dans la 1. version), l'IDEA (International Data Encryption Algorithm (clé de 128 bits)) et le RSA (Rivest, Shamir et Adleman (clé de 429 bits)).

Nous ne pouvons ici développer tout le débat sur la légalité de l'encryptage, souvent combattu dans la mesure où il rend impossible toute mesure d''écoutes'' des messages par l'autorité publique ou judiciaire.

[29] C'était le système utilisé par J. Helsingius avec son célèbre ''anon.penet.fi'' serveur (cf. http://www.penet.fi/injure.html). Sur les limites de ce système, consulter le Nymserver à l'adresse http://nymserver.com:Edtec.'' FaqEdTecAnonymous. Message.Remailer.

[30] J. Delmotte, M. Totori, C. Van Vaerenberg, *Internet et Vie privée*, Travail de fin d'études réalisé pour le DES en droit et gestion des Technologies de l'Information et de la Communication, FUNDP, Namur, avril 1997.

[31] J. Delmotte, M. Totori, C. Van Vaerenberg (*op. cit.*) présentent le système comme suit: ''L'utilisateur doit dans ce cas-ci encrypter son message. D'abord il applique la clé publique du destinataire sur le message vierge. Ensuite il chiffre le bloc qu'il a ainsi obtenu avec la clé publique du dernier serveur de remail dans la chaîne avant d'avoir inclus dans le bloc éventuellement des insctructions pour le dernier serveur. Pour chacun des serveurs qui se trouvent dans la chaîne en amont, l'utilisateur fait la même chose. Normalement, le nombre de serveurs qu'on utilise ne dépasse pas le nombre de trois, puisque le risque que le message sera perdu à cause d'un serveur en panne augmente''.

[32] Le système des ''Mixmasters'' est encore plus sure. Le message est réparti en plusieurs blocs de taille identique, ce qui conduit à l'impossibilité pour les hackers d'intercepter le message entrer (cf. cependant, L. Cottrell, Mixmaster and Remailer Attacks, http://www.obscura.com/rloki/remailer.essay.html).

[33] Pour plus d'informations, lire Anonymiser FAQ: http://anonymiser.cs.emu.edu:8080/faq.html.Ces services d'anonymisation sont proposés par l'opérateur public hollandais.

L'utilisation de ces systèmes soulèvent certaines questions

1. Comment est-ce que l'utilisateur du service d'anonymisation peut être sur que le serveur d'anonymisation ne garde pas de ''logs'' qui permettent de le tracer? Il faudrait en fait une autorité publique dans laquelle les utilisateurs peuvent avoir confiance (ex. les Certification Authorities (voir infra)).

2. Sur le plan technique, les logiciels d'anonymisation contiennent toujours des bugs, de façon qu'il n'est pas du tout exclu qu' un serveur contacté connaitrait l'identité des utilisateurs.

3. Le fournisseur d'accès garde une trace de votre identité.

B. *Les protections contre les traitements invisibles*

25. Certains logiciels installés dans le navigateur permettent soit de refuser systématiquement toute information excèdant la réponse à la requête de l'utilisateur et donc les cookies [34], soit d'alerter l'utilisateur de l'envoi de ceux-ci par un serveur contacté et de lui permettre de s'opposer à sa réception [35].

C. *L'information préalable sur les pratiques du serveur et les préférences de l'utilisateur en matière de vie privée*

26. Ce troisième type de solutions techniques poursuit un objectif différent des deux premiers types: il ne s'agit ni de protéger la confidentialité d'un message ni de lutter contre des traitements invisibles mais, d'une part, de permettre à l'utilisateur de sélectionner les sites visités après lui avoir donné une information sur les pratiques du serveur et d'autre part, le cas échéant, de permettre à l'utilisateur d'indiquer au serveur quelles conditions relatives à la protection de ses données il entend voir respecter.

Ces solutions encore à l'état de prototypes [36] s'avèrent prometteuses. Elles se fondent sur l'utilisation de technologies proches ou complémentaires de celles utilisées dans le cadre de la "Platform for Internet Content Selection" (PICS) [37], développée par le World Wide Web Consortium [38].

27. Le contexte du développement des PICS mérite d'être rappelé. Il indique, comme nous le dirons plus loin, les limites de leur utilisation au problème de la protection des données. Il s'agissait, en l'occurrence, de permettre aux parents de protéger les enfants mineurs contre l'accès à des sites pornographiques, de violence, etc. La technologie se fondait sur la "labellisation" des sites, généralement pratiquée par le site lui même. Le parent présélectionnait sur son ordinateur les critères d'accès aux sites et le navigateur automatiquement repérait les labels des sites. Si ceux-ci ne correspondaient pas aux critères de choix de l'utilisateur, l'accès au site était automatiquement réfusé [39].

28. L'idée des promoteurs de l'utilisation de la technologie PICS à la question de la protection des données repose sur des principes semblables:

[34] A ce propos, le message écran de la version démo du logiciel NS Clean 32.

[35] A ce propos, copie de l'écran du cookie Alert de Netscape 3.0.
La même fonctionnalité est offerte par le Microsoft Explorer sous le menu View Options/advanced/" Wam before accepting cookies".

[36] A ce propos sur l'état d'avancement de ces solutions, L.F. Cranor, art. cité et J. Reidenberg, *Governing networks and cyberspace Rule-making*, à paraître in *Emory Law Journal*, 1997, ...

[37] Sur la description de la norme et les graphiques illustrant son fonctionnement, http://www3.org/pub/WWW/PICS/principles/html.

[38] A propos de cette technologie, P. Resnick, J. Miller, *PICS: Internet Access Controls without Consorship*, Comm. of the ACM, 39(10), 87-93, 1996 et de son application à la privacy, P. Resnick, *Privacy Application of PICS*, Paper prepared for the Federal Trade Commission Public Worskshop, on Consumer Privacy on the G.I.I., June 4-5, 1996, disponible à l'adresse suivante http://www/research.att.com/~presnick/papers/ftc96/testimony.htm. Le développement de la technologie PICS est encouragée par la création aux Etats Unis d'un Technology Fund crée par la SEC. 552 du Telecommunications Act de 1996 (Pub. Law N. 104-104 Stat 56 (1996) Titre V Obscenity and Violence. En Europe, la Communication de la Commission sur le contenu illégal et dommageable sur Internet préconise également son adoption et sa diffusion à large échelle.) COM (96) 487 final).

[39] Dès décembre 1996, le Microsoft Internet Explorer 3.0. supportait la norme PICS. Cf. également la version 3.0. de Netscape.

— création d'une terminologie et d'un vocabulaire adéquats pour la description des pratiques de protection des données suivies par les organisations collectives de données [40];

— mise sur pied d'un audit pour "labelliser" suivant les critères retenus, les différents sites; cette "labellisation" peut être le fait du site lui-même, ou d'autorités indépendantes [41];

— possibilité a pour l'utilisateur de fixer ses propres exigences et dès lors de bloquer l'accès aux sites pour les serveurs qui ne répondent pas à ses exigences. On peut songer également à des possibilités de négociation au cas où le site Web n'offrirait pas a priori la protection désirée.

Cette négociation est particulièrement séduisante dans la mesure où elle permettrait à l'utilisateur d'indiquer au site visité les raisons pour lesquelles l'utilisateur ne désire pas aller plus loin que la page de bienvenue d'un site et d'ainsi, à terme, influer sur les pratiques de ce site en matière de protection des données.

Ainsi, si le serveur pouvait, au vu des préférences exposées par le navigateur [42], décider de répondre aux demandes de l'utilisateur [43] voire proposer à l'utilisateur de s'engager malgré tout dans les transactions proposées [44] [45].

29. L'énoncé de tels principes montre clairement l'intérêt [46] mais également les limites de l'application du système PICS au domaine de la protection des données.

En matière de pornographie ou de contenu à caractère racial ou violent, le système PICS permet à l'utilisateur de mieux connaître les pratiques non illégales d'un serveur et de se décider librement en connaissance de cause. En matière de vie privée, la réglementation de protection des données fixe l'obligation des collecteurs de données de respecter certaines pratiques. S'il existe, à partir de ce noyau dur, une marge de liberté pour assurer une plus ou moins grande protection, celle-ci est cependant loin d'être totale. Ainsi, le traitement des données sensibles est soumis à de

[40] Lors de leur brillant exposé devant le groupe de Berlin (Paris, avril 1997) J. Reidenberg et L.F. Cranor, montrèrent comment le modèle de code de conduite adopté par la Canadian Standard Institute pouvait être un point de départ de cette terminologie.

[41] ... qui bien entendu, devraient s' identifier. On peut songer aux autorités de protection des données. Le système de certification "volontaire" mis en place par le Code de conduite "Privacy" du Canadian Standard Association qui prévoit la possibilité d'audit des pratiques "Vie privée" des organisations et entreprises trouverait ainsi une application particulière.

[42] Ces préférences pourraient par exemple porter sur la durée de conservation, la non cession des informations personnelles à des tiers, etc...

[43] A propos de ce scénario qualifié de "Perfect Match", lire le Statement du Center for Democracy and Technology (CDT) devant la Fed. Trade Commission lors du Workshop on Consumer Privacy on the Global Information Infrastructure, Washington, June 4-5, 96.

[44] Dans ce second scénario qualifié par le CDT de "Mismatch", le serveur pourrait ainsi connaître des informations sensibles sur les détenteurs de systèmes de navigation, en l'occurrence leurs préférences en matière de privacy.

[45] D'autres extensions du PICS sont proposées: ainsi, la spécification des conditions de transfert automatiques d'informations de type particulier, c'est-à-dire celles strictement nécessaires à la conclusion de la transaction voire celles nécessaires à l'offre d'un service adapté à la personnalité de l'utilisateur. Ce transfert ne serait fait qu'à des sites dont les pratiques "Privacy " seraient conformes à l'attente de l'utilisateur. Le CDT (art. cité, p. 23 et s.) y voit aussi une manière pour les parents de protéger la vie privée de leurs enfants (Protecting Children's Privacy Online).

[46] ... intérêt salué par le groupe de Berlin "The Working Group would endorse a study of the feasibility to set up a new procedure of certification issuing" quality stamps "for providers and products as to their" privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighways" (Berlin Memorandum).

strictes conditions et le consentement des utilisateurs ne dispense pas les responsables de traitement de poursuivre des finalités légitimes.

30. Cette différence essentielle a un corollaire: en matière de contenu "indécent, violent, racial, etc.) le "rating" d'un site n'a rien d'obligatoire. En matière de protection de données, si on peut concevoir que le "rating" n'est pas obligatoire, il faudra cependant que certains critères du "rating" soient observés par tout serveur. La "protection des données" n'est point totalement négociable [47] [48].

L'affirmation témoigne clairement des limites de l'autorégulation, en même temps que du support indispensable que cette autorégulation apporte à l'effectivité d'un système réglementaire. Dans le monde d'Internet, une réglementation n'a de chance de se voir respectée que si elle trouve, par le biais de la technologie, des possibilités pour les utilisateurs de "contrôle" immédiat de son respect.

Section 2: *La solution réglementaire: de quelques questions relatives à l'application de la directive 95/46 au contexte d'Internet* [49].

31. Notre propos n'est pas d'analyser de manière exhaustive les dispositions de la directive mais de signaler quelques conséquences et difficultés majeurs de l'application de la directive au contexte d'Internet. Ainsi, nous nous centrerons sur les trois points suivants:

— le premier est l'analyse de certaines définitions qui délimitent le champ d'application matériel de la directive;

— le deuxième examine la portée territoriale de la directive;

— le troisième s'attache à l'examen de principes fondamentaux de la directive relatives aux limites des traitements de données.

A. *Le champ d'application matériel de la directive*

32. L'analyse de deux notions retiendra notre attention:

— la première est celle des "données à caractère personnel ", c'est-à-dire, selon l'article 2 a, de données [50] qui se rapportent à une personne physique, identifié ou identifiable. Cette notion trouve certainement à s'appliquer aux adresses électroniques personnalisées reprenant certains éléments relatifs à l'identité de leurs titulaires. Sans doute, s'appliquerait-t-elle également aux données de routage aux empreintes électroniques laissées lors de l'utilisation de services présents sur le Net, dans la mesure où des moyens d'identification existent et sont à la portée du détenteur de la donnée [51].

Si l'extension de la notion pose peu de problème d'interprétation, on peut s'interroger sur la pertinence de cette notion dans le contexte d'Internet. Un serveur peut, sans jamais chercher à connaître l'identité de l'utilisateur, disposer de nombreuses informations liées à l'adresse électronique voire IP de cet utilisateur et profiler ses services ou les services d'autrui en fonction du profil type de celui-ci. La simple donnée "adresse IP" ou "adresse électronique" ne mérite-t-elle pas dès lors protection, même s'il est prouvé que le serveur n'entend pas ou ne peut pas [52] identifier la personne disposant de cette adresse? La question mérite attention l'identification d'une personne se réfère t'elle au nom de la personne? Ne peut-on considérer qu'à travers une adresse et le profilage de l'utilisateur qui se cache derrière cette adresse, il s'agit également d'une identification de la personne? ou, sans se prononcer sur la nature personnelle ou non de la donnée, exiger, eu vu des risques de réidentification, la démonstration par l'opérateur du site que son système présente les garanties "appropriées" de non identification des personnes concernées.

33. La seconde est celle de "*traitement*". La notion de traitement est large et vise toute opération depuis la collecte jusqu'à la communication. L'application des dispositions de la directive à des opérations de simple consultation de site pose difficulté.

Faudra-t-il chaque fois, qu'il y a consultation de données nominatives sur Internet même sans stockage, ni copiage avertir les personnes concernées et leur ouvrir un droit d'accès à une donnée qui in casu n'est conservée que dans la mémoire humaine!

Une interprétation fondée sur le texte de la directive permet d'éviter une telle conséquence: au terme de l'article 2 b., la consultation n'est pas envisageable en tant que telle mais comme un élément d'un traitement, c'est-à-dire comme la possibilité offerte par le traitement de laisser consulter les données [53].

B. *Le champ d'application territorial de la directive*

— *le champ d'application « normal » de la directive*

34. La directive est applicable à tout traitement dont le responsable est localisé sur le territoire d'un des pays de l'Union européenne [54]. Un tel critère de rattachement est particulièrement idoine en matière de protection des données. Dans la mesure où un site peut être "logé" sur n'importe quel ordinateur situé sur le réseau, le

[47] A propos de la conciliation possible de la technologie PICS et des exigences réglementaires, lire les intéressantes propositions faites par J-M. Dinant in Using PICS as an enhanced privacy protection technology? disponible à l'adresse suivante http://www.det. fundp. ac. be/~jmdi L'idée essentielle est de développer un European Privacy Compliant Label qui serait géré par une autorité en lien avec les Commissions de protection des données et qui délivrerait le label aux sites qui se déclareraient conformes aux exigences de ce label.

[48] Une place pourrait être laissée à la négociation à partir de ce respect général de la directive. Ainsi, l'internaute pourrait négocier la durée de conservation de données, leur non communication à un tiers, le non profilage de clientèle, etc.

[49] Le lecteur se référera pour ce faire à l'analyse plus complète proposée par C. de Terwangne et S. Louveaux, *Data Protection and on-line networks*, Computer Law and Security Report, 1997, à paraître. Certaines idées exposées ci-dessous sont reprises de l'analyse proposée par ces auteurs.

[50] ... qu'il s'agit de textes, de sons ou d'images. Cette précision est importante dans la mesure où Internet devient de plus en plus un réseau multimédia (ex. mise sur le réseau d'un curriculum vitae avec photo du candidat).

[51] Cf. le considérant n. 26: "... pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne".

[52] Le considérant 26 souligne que les moyens doivent être susceptibles d'être mis en œuvre et non être effectivement mis en œuvre.

[53] A propos de cette interprétation, M-H. Boulanger, C. de Terwangne, *Internet et le respect de la vie privée*, in *Internet face au droit*, E. Montero (éd.), Cahier du CRID n. 12, Bruxelles, Story Scientia, 1997, p. 211.

[54] Sans doute, faudrait-il prévoir comme le font les réglementations de protection des consommateurs en matière de ventes à distance, l'obligation pour tout site d'identifier clairement le responsable du site, son adresse et sans doute les finalités de la collecte d'informations personnelles.

critère du responsable c'est-à-dire de celui qui définit les finalités et les moyens du traitement présente plus de stabilité [55].

La difficulté demeure lorsque le responsable et son adresse ne peuvent être identifiés [56]. Une solution pourrait être alors de rendre responsable celui qui assure la maintenance du site en question en localisant la machine où est situé le site [57].

La localisation du responsable soulève d'autres difficultés: une simple adresse électronique est rarement parlante quant à la localisation d'un site [58]. En outre, qui est responsable d'un forum de discussion? Si on considère que c'est le modérateur, faut-il se fixer en ce qui concerne la loi acceptable, à l'adresse de son établissement.

— la portée internationale de la directive

35. Selon l'article 4 c) de la directive, le droit national pris en application de la directive s'applique: "lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire dudit Etat membre". L'article 4.2. ajoute que l'applicabilité du droit national entraîne l'obligation pour le responsable de désigner un représentant établi sur le territoire de l'Etat membre [59].

36. Le critère de rattachement affirmé par le texte est donc le "recours" à des moyens automatisés ou non situés sur le territoire de l'Union européenne. La notion est vague. Prise au sens large, elle consacrerait des hypothèses où la collecte des informations opérée par exemple en Belgique est suivie par un transfert des données vers l'étranger pour y être traitée par exemple à meilleur prix mais également l'interrogation d'une banque de données sise en Belgique, dans la mesure où l'interrogation s'opère suivant un logiciel propre à la banque de données. Elle étendrait même l'applicabilité de la directive à un système de réservation aérienne dans la mesure où interrogeant une boite aux lettres tenue à sa disposition en Europe par une agence de voyage, il prend connaissance de messages EDI qui lui sont destinés. Appliquée à Internet, une telle interprêtation permettrait de considérer que toute personne qui interroge un site européen et télédécharge des données nominatives à partir de son interrogation recourt à des moyens automatisés situés sur le territoire de l'Union Européenne et se voit donc appliquée la directive.

Bref, l'interprétation large de la notion de "recourir" aboutirait à décréter que la quasi totalité des flux transfrontières générés par Internet amènerait le destinataire des flux à tomber sous le champ d'application de la directive. Point ne serait besoin

[55] Cf. à ce propos, la définition donnée par l'article 2 d de la directive. L'article 4 1 a) de la directive ajoute que si le responsable dispose de plusieurs établissements sur le territoire de plusieurs pays de l'Union, il doit observer les droits nationaux des divers pays des établissements. A notre avis, le fait que le site d'un responsable est consultable de divers pays de l'Union Européenne ne conduit pas à affirmer la pluralité d'établissements. La notion d'établissement se réfère (considérant n. 11) à une installation stable, ce qui n'est pas le cas ici.

[56] Sans doute, faudrait-il prévoir comme le font les réglementations de protection des consommateurs en matière de ventes à distance, l'obligation pour tout site d'identifier clairement le responsable du site.

[57] On est conscient du fait que cette machine peut être une simple boîte postale électronique où est hébergé temporairement le site.

[58] A ce propos, M-H. Boulanger, C. de Terwangne, o.c., p. 201.

[59] Auprès duquel s'exerceront notamment les droits d'accès, d'opposition, et de rectification.

alors des dispositions des articles 25 et 26 de la directive, puisqu'en toute hypothèse la directive serait applicable.

37. Lors d'une analyse récente de l'application de la directive à Internet, M-H. Boulanger et C. de Terwangne [60] ont proposé une autre interprétation qualifiée de "téléologique" du critère de rattachement proposé par l'article 4.1.C). Nous en reproduisons le texte: "La ratio legis de cet article se résume clairement dans la volonté d'éviter que les individus se trouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la directive, même en dehors des frontières communautaires.

C'est par une lecture combinée de l'article 4.1.c et des articles 25 et 26 qui régissent les flux transfrontières vers les Etats tiers qu' une définition rationnelle de l'applicabilité de la directive pourra être dégagée.

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communauté. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à l'étranger en provenance de l'Union est exigée".

38. La réponse contenue dans l'article 4.1.c. vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manoeuvre artificielle, du bénéfice de la protection de l' ensemble de la directive, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 4.1.c:

— celle précisément où un responsable de traitement cherche délibérement à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire communautaire pour réaliser son traitement. Par exemple, le cas d'un serveur d'annuaires téléphoniques reprenant les abonnés italiens et dont la cible commerciale est purement ou en tout cas majoritairement européenne mais qui pour éviter les réglementations européennes s'installerait au Maroc.

— celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. A notre avis, cette situation vise les collectes de données personnelles réalisées par le biais de cookies introduites dans le système d'informations de l'utilisateur et à son insu. Dans un tel cas, le responsable du site « recourt » à des moyens électroniques situés dans le pays de l'utilisateur [61].

Elle pourrait également viser une collecte opérée à partir de l'étranger par le biais d'un logiciel qui visiterait l'ensemble des forums de discussions mis en place par des serveurs européens et d'y repérer les interventions de telle ou telle personne afin de constituer son profil de personnalité.

[60] M-H. Boulanger, C. de Terwangne, o.c., p. 202. Les auteurs se réfèrent également à la lecture du considérant n. 20 et à l'exposé des motifs de la première proposition de directive émanant du Conseil (Proposition du 15 oct. 1992, COM(92) 422 final - SYN 287, p. 13).

[61] M-H. Boulanger et C. de Terwangne (o.c., p. 210) considère que le même raisonnement s'applique dans le cas de l'enregistrement de données de routage, c'est à dire selon les auteurs dans le cas de flux actifs cachés", Flux actifs dans la mesure où ils sont initiés par une action de la personne concernée.

Par contre, il apparaît peu raisonnable de considérer que suite à l'envoi conscient par un utilisateur d'un message à un site hors Europe, ce site tombe sous le champ d'application de la Directive. Dans un tel cas, il y a transmission de données nominatives vers un pays tiers et les dispositions des articles 25 et 26 s'appliqueront (infra, n. 36).

39. En conclusion, l'article 4.1.c) viserait des hypothèses exceptionnelles soit celle où la localisation du responsable est anormale au regard de son autorité orientée vers l'Union européenne et déterminée par des données en provenance de celle-ci, soit celle où est déjouée la protection offerte par la réglementation des flux transfrontières dans la mesure où ce flux est généré par la seule activité de la personne située à l'étranger sans qu'il y ait à proprement parler communication c'est-à-dire action consciente de transfert de données, d'un responsable de traitement situé dans le territoire de l'Union européenne.

— *les flux transfrontières*

Le principe: la nécessité d'une protection adéquate [62]

40. En vertu de l'article 25.1. de la directive, "les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat". Le principe est donc l'interdiction du transfert, sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation [63] du caractère adéquat de la protection du pays tiers doit tenir compte de "toutes les circonstances relatives à un transfert ou à une catégorie de transferts" et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et certains concernent le niveau de protection dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées".

41. Au-delà de ces réflexions, la notion de "protection adéquate" conduit à une approche - qui, à la lecture du texte de l'article 25, se caractérise comme suit:

— *une approche au cas par cas* [64], c'est-à -dire que la situation de la protection des données dans un pays tiers est évaluée "par rapport" à un transfert déterminé ou une catégorie de transferts". L'instrument méthodologique doit caractériser de manière précise le cas visé;

— *une approche souple et ouverte* puisque selon le libellé même de l'article 25.2 l'évaluation doit pouvoir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque Etat, voire chaque responsable des données, peut apporter, l'article 25 § 2 étant purement indicatif à ce propos;

— *une approche fonctionnelle*, c'est-à-dire que la protection s'évalue tant *par rapport aux risques* d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

42. L'évaluation de ces mesures doit se faire sans a priori; il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d'impéralisme européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ de la directive. Au contraire, elle crée pour l'évaluateur la nécessité, tout en ne perdant pas de vue les exigences qui fondent selon la directive le besoin de protection, de prendre en considération les adaptations originales des modalités de cette protection, adaptations proposées par les pays tiers. Il s'agit de rechercher s'il y a "similarité fonctionnelle" [65].

43. Quelques remarques liminaires s'imposent d'emblée au sujet de la notion d'« adéquation », que d'aucuns ont opposé à celle d'équivalence" [66].

— Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question: « par rapport à quoi la protection doit-elle être adéquate »?). Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer, la protection du pays tiers.

— Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut « en particulier » prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

— Troisièmement, le contenu de ces éléments n'est pas défini: si par exemple on sait qu'il faut prendre en compte la durée des traitements, la directive n'indique pas plus avant ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devraient être le « contenu minimum » d'une législa-

[62] Sur l'étude de cette notion, B. Havelange, Y. Poullet, (avec la collaboration de M-H. Boulanger, H. Burkert, C.de Terwangne, A. Lefebvre), *Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel*, Exec. Summary, Etude réalisée pour la Commission des Communautés européennes, février 1997, à paraître.

[63] De qui relèvera l'appréciation du caractère adéquat? Quel rôle joueront dans cette procédure, les autorités nationale de protection des données?

[64] Par opposition à une approche légistique qui se fondrait sur une comparaison des textes.

[65] La "similarité fonctionnelle" implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si les dits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète, législative en tout cas.

[66] La notion de protection équivalente est utilisée par la Convention du Conseil de l'Europe, dite Convention n. 108 en son article 12. Cet article met à charge d'une partie contractante une obligation de permettre les flux vers les autres Etats partie à la même convention si cet Etat assure une protection équivalente. On notera que la notion d'équivalence de protection ne règle que les flux entre pays ayant ratifié la Convention du Conseil de l'Europe et non vers les pays tiers.

A propos de cette différence, A. Bourlond, Y. Poullet, *Flux transfrontières de données à caractère personnel, position de la proposition de directive européenne face à celle de la convention 108 du Conseil de l'Europe*, D.I.T., 1991/2, p. 58 et s.

tion ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection. On ajoutera que certains éléments énoncés se réfèrent aux caractéristiques du flux et désignent des facteurs de risques, alors que d'autres désignent la qualité des instruments de protection mis en place dans le pays tiers.

44. Enfin, à propos des instruments de protection mis en place, l'article 25 se réfère non seulement aux normes issues de l'autorité publique qu'elles soient générales ou sectorielles [67] mais également à des codes de conduite [68] voire à des mesures techniques pourvu que ces instruments soient "respectées". Ainsi l'autorité de protection sera plus attentive à l'effectivité d'un instrument, qu'à sa nature: ce qui importe, c'est qu'elle soit convaincue que l'instrument — même s'il s'agit d'une simple "Company Privacy Policy" — soit largement diffusé parmi les personnes concernées et les responsables des fichiers et puisse faire l'objet de recours des premiers vis-à-vis des seconds en cas de non respect par ceux-ci.

45. L'article 25 al. 1 et al. 2 consacre, nous l'avons dit, une approche au cas par cas, flux par flux ou catégorie de flux par catégorie de flux. Une telle analyse est évidemment lourde pour les Etats membres et les articles 25.4. et 25.6. mentionnent deux possibilités pour la Commission de leur simplifier le travail. Il s'agit de constater "conformément" à la procédure prévue à l'article 31 § 2 qu'"un pays tiers assure ou n'assure pas un niveau de protection adéquat". En d'autres termes, ces paragraphes permettent la constitution de "white" ou de "black" lists, décision valable pour des catégories de transferts, pour un secteur voire pour l'ensemble des flux vers un pays tiers [69].

46. La directive,"sous réserve de dispositions contraires de leur droit national régissant des cas particuliers "[70], édicte certaines exceptions au principe de l'article 25 et autorise ainsi des transferts de données à caractère personnel vers des pays

[67] Ainsi, une législation sur le secret médical pourrait garantir adéquatement dans le secteur médical, la protection des données.

[68] La Canadian Standard Association a établi un code de conduite modèle en matière de respect de la vie privée qui prévoit des mécanismes originaux de certification pour les entreprises par des organismes agréés et des recours possibles. A propos de ce modèle: C. Bennett, *Privacy Codes, Privacy Standards and Privacy Laws: the instruments for Data Protection and what they can achieve*, Paper presented at Visions for Privacy, Victoria, British Columbia, 9-11 mai, 1996.

[69] Analyse au cas par cas et analyse globale: les deux types d'analyse ne sont pas contradictoires. L'analyse globale suivra le plus souvent une série d'évaluations au cas par cas, éventuellement pratiquées par différents Etats Membres; elle pourrait également se déduire d'un système de protection générale des données dont le contenu, le contexte et l'application désignent à coup sûr comme adéquate ou inadéquate la protection offerte par les pays tiers.

[70] "Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat (...) peut être effectué (...) (Article 26.1). "Les Etats membres peuvent donc, par des dispositions régissant des cas particuliers, refuser que l'une ou l'autre exception s'applique à ces cas. On pense dans un premier temps aux situations mettant en jeu des données sensibles, médicales ou judiciaires. Mais la particularité des cas retenue peut être plus large et consister non plus dans le caractère sensible des données mais, par exemple, dans la nature du réseau — ouvert ou fermé — utilisé. On peut donc imaginer qu'un Etat membre soit plus strict qu'un autre en matière d'exceptions appliquées à l'utilisation d'un réseau Internet" (M-H. Boulanger, C. De Terwangne, *Internet et le respect de la vie privée*, in Internet face au droit, E. Montero (éd.), Cahier du CRID n. 12, Bruxelles, Story-Scientia, 1997, p. 211). L'interprétation donnée par les auteurs cités est ainsi large. La notion de "cas particulier" pourrait s'interpréter comme laissant seulement la possibilité pour l'autorité nationale d'intervenir pour un flux déterminé et de déroger exceptionnellement et non par catégorie aux différentes hypothèses prévues par l'article 26.

n'offrant pas un niveau de protection adéquat. Deux types d'exception sont prévus: le premier vise certaines catégories de flux; le second vise la substitution à un mode adéquat de protection, d'un mode "ad hoc" de protection: le contrat.

47. A propos de la première catégorie d'exceptions, l'article 26.1 vise notamment les hypothèses où la personne concernée a indubitablement donné son consentement à l'opération de transfert (article 26.1a). On ne peut parler de véritable consentement que si celui-ci est "éclairé" c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données.Cette première exception se révélera utile dans le cadre d'Internet dans la mesure où le consentement pourra être demandé et obtenu directement via le réseau. D'autres exceptions existent. Elles reprennent en gros les hypothèses prévues par l'article 7 de la directive pour légitimer un traitement tantôt le transfert est nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles, soit entre la personne concernée et le responsable du traitement, soit entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée [71], tantôt le transfert sert à la sauvegarde d'un intérêt vital ou d'intérêt public important ou s'opère dans le cadre d'une action en justice [72].

48. La seconde catégorie d'exceptions substitue à des modes adéquats de protection, ceux palliatifs envisagés par le responsable dans le cadre d'un flux ou de plusieurs flux pour garantir le respect de la protection des données. Les clauses contractuelles en particulier [73] sont visées. Ainsi, si le secteur marketing d'un pays tiers n'offre pas de protection adéquate aux données originairement protégées par la Directive, une entreprise (ou l'association des sociétés de marketing) peut prendre dans le cadre des contrats couvrant les flux transfrontières en provenance d'Europe, des engagements supplémentaires, par exemple limitant les finalités de réutilisation des données, ouvrant le droit d'opposition et finalement permettant à une autorité de protection des données d'inspecter leurs traitements [74].

C. *De quelques principes de base de la directive*

49. Internet représente à la fois un outil de collecte d'informations mais également de communication entre la personne concernée et le responsable du traitement.

[71] Ainsi par exemple un service de réservation aérienne transmettra à des agences locales de voyage le nom des voyageurs désirant réserver un hôtel.

[72] L'article 26.1 6) ajoute le cas d'un transfert à partir d'un registre public "destiné réglementairement à l'information au public et ouvert à la consultation" (ainsi, par ex., le registre du commerce).

[73] A l'appui d'un contrat, des mesures techniques ad hoc pourraient également être envisagées pour constituer une garantie suffisante. Sur les contrats, comme modèle supplétif d'assurer une protection équivalente ou adéquate dans les flux transfrontières, C.M. Pitrat, *Clauses modèles pour les flux transfrontières de données ou comment assurer une protection équivalente*, DIT, 1993/1, pp. 46 à 52; L. Early, *Securing equivalent protection among nations in the context of TBDF: a possible role for contract law*, DIT, 1990/4, pp. 10 et s. Le lecteur trouvera dans ces écrits des références aux clauses modèles élaborées conjointement par le Conseil de l'Europe et la CCI (Strasbourg, 2/11/92, T.PD(92) 7 revised).

[74] A propos de ce second type d'exception, une autorisation de l'Etat membre sera nécessaire. Elle supposera le caractère "suffisant" des garanties offertes. L'Etat membre devra informer la Commission de telles autorisations et des oppositions exprimées par d'autres Etats membres seront possibles. On souligne à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des Etats membres, imposer une décision aux Etats membres, soit l'acceptation de telles mesures palliatives, soit leur rejet ou la proposition de mesures supplémentaires.

Cette double fonction présente dans un même média permet de rendre plus effectives certaines dispositions de la directive. On songe en particulier à la manière dont le principe de transparence, les droits d'accès, de correction pourraient s'exercer via Internet et à moindre coûst. Au-delà, la configuration des écrans pourrait permettre à l'internaute de connaître à tout moment l'identité du responsable, les finalités poursuivies par celui-ci voire, via un lien html, les dispositions réglementaires ou autoréglementaires que le responsable s'engage à suivre [75].

L'interactivité du média ouvre d'autres possibilités encore, possibilité de déterminer les utilisations de données, auxquelles l'utilisateur consent, et ce en cochant des cases apparaissant à l'écran avant la collecte des données, possibilité d'exercer a priori son droit d'opposition, etc..

50. Le consentement reçoit, dans le contexte d'Internet, une portée et une efficacité nouvelle. On pourrait être tenté d'y voir une base de légitimité suffisante pour les traitements de données collect ées via Internet. En ce sens, on relève une disposition d'un projet de loi allemand, qui considère le consentement comme fondement suffisant d'un traitement effectué on line suite à l'utilisation d'un service disponible.

Nous pouvons difficilement accepter un tel raisonnement. Outre que le consentement risque de ne point être libre et éclairé, il ne dispense pas d'un examen de la légitimité du traitement [76]. Certes, cet examen se fondera sur une appréciation marginale dans la mesure où le consentement au traitement crée une forte présomption, mais une telle présomption pourrait céder devant une interdiction de l'Etat relative au traitement de certaines données [77] ou de certains traitements [78]. Par ailleurs, une action a posteriori des autorités judiciaires ou de contrôle pourrait considérer le traitement pourtant consenti comme illégitime.

51. Le principe de la collecte et du traitement loyal s'applique aux traitements réalisés via Internet. L'article 6.1. a de la directive qui exige que la collecte et l'utilisation de données soient faites de manière loyale exclut des pratiques comme celles dénoncées dans la première section à propos des traitements invisibles. "Personal Data may only be collected in a transparent way" [79].

52. On ajoutera enfin que selon l'article 6 1 b l'utilisation des données doit être "compatible" avec la ou les finalités annoncés lors de la collecte des données, c'est-à-dire rentrer dans le champ des utilisateurs raisonnablement attendus par la personne concernée à la lecture des finalités annoncées par le responsable du traitement.

[75] On pourrait même songer à voir appraître à l'écran les données relatives au traitement qui sont consignées dans le registre accessible au public, tenu par l'autorité de contrôle.

[76] Ainsi, on peut douter de la liberté de consentement du chercheur d'emploi, appelé à donner certaines données de son passé par un serveur ayant créé une banque de données de recherches d'emploi.

[77] La directive prévoit expressement la possibilité pour l'Etat de prévoir des exceptions en matière de données (art. 8 § 1 a). Le Budapest-Berlin Memorandum interdit la publication d'avis de recherche policiers sur Internet vu le manque de sécurité des procédures d'authentification et les possibilités de manipulation des images.

[78] Ainsi, en matière de videotex, les traitements d'analyse psychologique du comportement de l'utilisateur, lors de son utilisation de jeux video avaient été condamnés.

De même, les cablo-opérateurs américains se sont vus interdire sauf pour finalités d'analyse du marché l'enregistrement des choix de programmes réalisés par un spectateur. Par analogie, ne pourrait-on interdire ce type de traitement aux fournisseurs d'accès.

[79] C'est le Guidance 2 affirmé par le Budapest-Berlin Memorandum déjà cité.

Quelques exemples illustrent cette notion: en participant à un forum public de discussion relatif à la cryptographie, une personne peut s'attendre à ce que des invitations lui soient envoyées à propos de conférences ou séminaires en la matière; par contre le consommateur qui visite le site d'un supermarché sur Internet ne peut raisonnablement pas s'attendre à ce qu'une firme tierce sur base de l'analyse de son profil de personnalité lui propose l'achat d'ouvrages ou la participation à tel ou tel voyage, comme cela pourrait être le cas si les deux entreprises participent à un système commun d'analyse du comportement de l'utilisateur comme "double click".

L'Internaute qui accède au réseau via un fournisseur d'accès peut raisonnablement s'attendre à ce que ses données de connexion soient utilisées par le fournisseur d'accès pour que ce dernier lui propose des conditions spéciales mais non pour communication à des serveurs avec lesquels ce fournisseur entretient des relations privilégiées.

Conclusions

53. Le phénomène d'Internet interpelle l'honnête homme protecteur des données. La dimension internationale de ce réseau des réseaux contraint à la recherche de solutions sans frontières d'un consensus mondial. La construction de celui-ci sera tâche difficile même si certains éléments paraissent le faciliter.

Au premier rang de ces éléments, sans aucun doute la technologie. Si sans doute, elle est à l'origine de tous les risques, elle en est sans doute également le meilleur garde fou. Sans frontières, élaborée par des multinationales, elle apporte à l'internaute tout d'abord la possibilité d'une confidentialité de ses interrogations et de ses messages. Ensuite, elle crée, interactivité du réseau aidant, la chance unique d'une transparence du destinataire, c'est à dire du responsable des données, mieux d'un dialogue avec celui-ci par lequel il exprimera son choix ou son non choix en faveur de la protection des données.

Certes, la solution technologique ne s'impose pas, elle se conquiert : les multinationales qui la développeront ne le feront jamais que dans la mesure où la pression des utilisateurs rend nécessaire la stratégie d'un tel développement. Le lobby de la protection de la vie privée sera t'il suffisamment convainquant pour que les privacy enhancing technology existent ...et soient accessibles à l'utilisateur à un prix abordable. Ce slogan du service universel doit être rappelé ici. Sans doute, est-ce le rôle de l'Etat d'aider à la recherche-développement en la matière et à la diffusion de telles technologies.

54. Les technologies dites de promotion de la vie privée ont pour caractéristique de déplacer le centre de gravité en ce qui concerne l'acteur responsable de la protection des données et sans doute est-ce en la matière qu'Internet représente une vraie révolution dans le débat de la protection des données. Traditionnellement, dans nos démocraties européennes, la protection des données était confiée principalement à la loi et à l'autorité de contrôle que la loi instituait. La personne concernée intervenait peu dans sa propre protection. Certes dira t'on existe le droit d'accès mais les statistiques sont là pour témoigner de la faible utilisation de celui-ci. La technologie d'Internet offre à la personne concernée de devenir en ligne maître des choix qu'elle opère, ainsi de transmettre ou non telle ou telle information, de révéler ou non son identité, de sélectionner ou non les sites sur base de leurs pratiques en matière de protection des données et finalement de négocier avec le responsable sur ses « privacy preferences ».

... Qu'elle est précieuse cette responsabilité nouvelle de la personne concernée... Sans doute est-ce avec raison que les groupes de protection des données aux Etats Unis, comme le Center for Democracy and Technology, soulignent cet « *empowerment* » de la personne concernée. Que cette responsabilité nouvelle doive être cultivée et encouragée, cela va de soi. Qu'elle ne conduise pas à la conclusion à laquelle certains voudraient aboutir que l'intervention de la loi est désormais inutile. Le Droit ne peut se contenter de déplorer la difficulté de son application et d'affirmer que l'espace virtuel est désormais un espace sans droit ou plutôt conduit par la seule autonomie des volontés. Au contraire, le Droit doit trouver dans une expression normative plurielle la manière adéquate d'agir. Dans toute la mesure du possible, il renverra par l'application de principes généraux à des normativités présentes dans le réseau: l'application des principes sous forme d'autorégulation, la standardisation technique... Il puisera, le cas échéant, dans le contenu de cette réglementation interne au réseau, l'inspiration pour définir si possible au plan international, des règles de loi. Sans doute, s'agit-il, selon l'expression de M. Vivant, d'un droit post-moderne ou selon celle de J. Reidenberg, d'un nouveau « network governance paradigm ». Loin de consacrer la démission de l'Etat, ce droit « post moderne », ce « paradigme » nouveau invite-t'il à créer de nouveaux modes de dialogue entre diverses normativités techniques, éthiques et réglementaires et, tâche plus difficile, des instances démocratiques capables de susciter ce dialogue et de le mettre au service de l'intérêt général!

PAOLO CASELLA

Ringrazio il professor Poullet per la sua amplissima relazione su alcuni degli aspetti inquientanti di Internet. Si tratta, come abbiamo sentito, di strumenti che hanno la caratteristica di essere particolarmente subdoli, visto che spesso non sono controllabili o verificabili da parte dell'utente.

A proposito dei *cookies*, per esempio, piccoli programmi che hanno la funzione, come ci ha illustrato il professor Poullet, di trasmettere informazioni sull'utente, spesso senza che lui ne sia a conoscenza, occorre sottolineare che i programmi sull'utente, permettono la navigazione in Internet (i c.d. *browsers*), di norma consentono l'emissione di un segnale d'avvertimento quando il sito a cui si è collegati invia un *cookie*, ma sono predisposti all'origine in modo che l'avvertimento non venga trasmesso. Tocca all'utente, configurando il suo programma nel modo opportuno, attivare questa segnalazione. Attualmente, peraltro, sono disponibili in rete piccoli programmi gratuiti che hanno la specifica funzione di purificare un sistema dai *cookies* che sono presenti (es.: *Cookie Monster*).

L'argomento è affascinante, ma dopo l'ampia trattazione del professor Poullet possiamo senza dubbio passare alla successiva relazione. Lascio, quindi immediatamente la parola al professor Rodotà, il quale ha gentilmente dato la propria disponibilità a sostituire la professoressa Lenoir, che non è potuta essere con noi oggi. Il professor Rodotà ci parlerà de « Le informazioni genetiche ».